UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/629,853	07/30/2003	Kiyoshi Kohiyama	1341.1157	6150

21171 7590 04/05/2007

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
BLUDAU, BRANDON S	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/629,853	KOHIYAMA ET AL.	
	Examiner	Art Unit	
	Brandon S. Bludau	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-40 are pending.

Claim Objections

2. Claims 6,8,26 and 28 are objected to because of the following informalities: the claims state reading information on an "irregularly basis". The Examiner notes a grammatical error in that they should read: "on an irregular basis" Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1 and 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The preamble cites an information reproducing apparatus, however, there is no language in the claim directed to reproducing information.

4. Claims 10 and 30 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 10 recites changing original information, it is unclear to the examiner what is meant by "original information" and how this may differ over the language of claim 7. Same arguments apply to claim 30.

5. Claims 11 and 31 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 11, discusses "pre-updating information" and "post-updating information", there is no antecedent basis for this information in the claims. Moreover, the Examiner is uncertain what is meant by such pre and post updating information. Same arguments apply to claim 31.

6. Claims 18 and 38 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear what is meant by a normal information, and what the metes and bounds of this limitation are.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-2,5,17,20-22, 25,37 and 40 are rejected under 35 U.S.C. 102(b) as being anticipated by Jablon et al. (US Patent 5421006).

8. As per claim 1, Jablon discloses an information reproducing apparatus, comprising:

a secure module that stores a first information, wherein the secure module can not be accessed from outside (column 8 lines 39-41 wherein the secure module is the protectable non-volatile memory);

a memory that stores a second information, wherein the memory can be accessed from outside (column 8 lines 45-50); and

a falsification checking unit that is loaded on the secure module, wherein the falsification checking unit reads the second information from the memory by direct access, compares the second information with the first information in the secure module, and checks a falsification of the second information based on a result of the comparison (column 8 lines 39-68).

9. As per claim 2, Jablon discloses the information reproducing apparatus according to claim 1, wherein the falsification checking unit reads all of the second information (column 8 lines 63-64 wherein the modification detection code is computed over the entire second information).

10. As per claim 5, Jablon discloses the information reproducing apparatus according to claim 1, wherein the second information is software (column 8 lines 45-50).

11. As per claim 17, Jablon discloses the information reproducing apparatus according to claim 1, further comprising: a writing unit that is loaded on the secure module, wherein the writing unit writes a secret information within the secure module into the memory as the second information using the direct access method, wherein the falsification checking unit checks falsification of the second information based on

response information corresponding to the secret information (column 9 lines 13-20 and 19 lines 23-44).

12. Claims 20 and 21 are rejected because they disclose substantially similar subject matter to claim 1.

13. Claim 22 is rejected because it discloses substantially similar subject matter to claim 2.

14. Claim 25 is rejected because it discloses substantially similar subject matter to claim 5.

15. Claim 37 is rejected because it discloses substantially similar subject matter to claim 17.

16. Claim 40 is rejected because it discloses substantially similar subject matter to claims 1 and 21.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 3-4,6,18-19, 23-24,26 and 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon (US Patent 5421006).

18. As per claim 3, Jablon discloses the information reproducing apparatus according to claim 1, but does not explicitly disclose wherein the falsification checking unit reads a part of the second information. As discussed above, Jablon computes the

modification detection code over the entire second information, however, the Examiner finds it to be an obvious modification to one skilled in the art to compute the code over a part of the second information. Motivation as would have been readily apparent to one of ordinary skill in the art at the time of the invention would have been to reduce processing time by only having to compute a code over a smaller amount of data, as is commonly practiced in the art.

19. As per claim 4, Jablon discloses the information reproducing apparatus according to claim 1, but does not explicitly disclose wherein the falsification checking unit performs the comparison of the first information and the second information using a checksum method. Jablon does however discuss this method in the background (column 5 lines 26-35), and further provides the modification detection code as a superior alternative, thus it was well known and practiced in the art to perform such comparisons using a checksum method.

20. As per claim 6, Jablon discloses the information reproducing apparatus according to claim 1, but does not explicitly disclose wherein the falsification checking unit reads the second information from the memory on an irregularly basis. Jablon discloses the method wherein the second information is checked only prior to being executed, the Examiner could argue that the specific programs may be executed on an irregular basis determined by selection of the user or system, moreover, the Examiner argues that it is a design choice whether to compare data prior to execution of the code, periodically or irregularly. One of ordinary skill in the art would have found it an obvious modification to perform such a comparison on an irregular basis, motivation for doing so

would have been to continuously monitor system memory for corruption, not only upon execution of the code.

21. As per claim 18, Jablon discloses the information reproducing apparatus according to claim 17, but does not disclose wherein the secret information is stored in a controlled memory space, wherein the controlled memory space is such that a normal information is read out from the memory space at a first time and a different information is read out at a second time. The Examiner argues that it would have been an obvious modification to Jablon to include a controlled memory space for storing the secret information. Such memory spaces are commonly implemented in the art for enhancing security of the memory space, so as to obfuscate access to the secret information in the memory as is well known to one of ordinary skill in the art.

22. As per claim 19, Jablon discloses the information reproducing apparatus according to claim 1, but does not disclose wherein the second information is encrypted MPEG data. Moreover, the Examiner argues that while Jablon is directed to securing strictly programs, similar methods of data comparison are practiced for a multitude of applications. Thus it would have been obvious to implement the comparison method of Jablon to any embodiment that wishes to secure data especially encrypted MPEG data.

23. Claims 23-24 is rejected because they disclose substantially similar subject matter to claims 3 and 4 respectively.

24. Claim 26 is rejected because it discloses substantially similar subject matter to claim 6.

25. Claims 38-39 are rejected because they disclose substantially similar subject matter to claims 18 and 19.

26. Claims 7-11 and 27-31 are rejected under 35 U.S:C. 103(a) as being unpatentable over Jablon (US Patent 5421006) in view of Osborn (US Patent 6026293).

27. As per claim 7, Jablon discloses the information reproducing apparatus according to claim 1, but does not explicitly disclose the method further comprising: an updating unit that is loaded on the secure module and that updates the second information in the memory using a direct access method, wherein the falsification checking unit reads the second information updated by the updating unit.

Osborn discloses a similar method of checking for data integrity by comparing a previously authenticated hash value in protected memory to a newly computed hash value. Osborn discloses a method of updating the second information and performing a comparison on the updated information (see column 7 lines 4-12). It would have been obvious for one of ordinary skill in the art to modify Jablon to include a means for updating a second information and forming a comparison on the updated information. Motivation for modifying Jablon as discussed above would have been obvious to one of ordinary skill at the time of the invention, so as to enable a device to modify contents in memory wherein a comparison step necessarily checks for integrity of the newly modified data. Moreover Osborn discusses this enhancement for the reprogramming of a memory for the device (column 7 lines 4-5).

28. As per claim 8, Jablon in view of Osborn discloses the information reproducing apparatus according to claim 7, but does not disclose wherein the updating unit updates

the second information on an irregular basis. The Examiner argues this to be an obvious modification, if not a mere design choice. Based on Jablon or Osborn, it would have been obvious to include wherein updating of information in a memory is done on an irregular basis, for either a random reprogramming of memory or reconfiguration of code in memory. Motivation for doing so would have been a continuous updating of a profile information or a subscriber number as would have been obvious in view of Osborn. Moreover, It would have been recognized as a design choice when to update the contents in a memory, as would have been readily apparent to one of ordinary skill in the art at the time of the invention.

29. As per claim 9, Jablon in view of Osborn disclose the information reproducing apparatus according to claim 7, wherein the updating unit updates a part of the second information (Osborn column 7 lines 10-12 wherein any modification, whether it be of a complete information or part of an information is necessarily discussed).

30. As per claim 10, Jablon discloses the information reproducing apparatus according to claim 1, but does not explicitly disclose the method further comprising: a storage control unit that is loaded on the secure module, wherein the storage control unit changes original information, and stores the changed information as the second information into the memory. Osborn does disclose such a method wherein a storage control unit changes original information and the stores the changed information as the second information. The same arguments as applied to claim 7 are applied here.

31. As per claim 11, Jablon in view of Osborn discloses the information reproducing apparatus according to claim 10, wherein when the second information is updated, the

storage control unit hands over the second information from the pre-updating information to the post-updating information (column 7 lines 4-12).

32. Claims 27-31 are rejected because they disclose substantially similar subject matter to claims 7-11 respectively.

33. Claims 12 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon (US Patent 5421006) in view of Osborn (US Patent 6026293) and further in view of Asokan et al. (US PgPub 2003/0076957).

34. As per claim 12, Jablon in view of Osborn disclose the information reproducing apparatus according to claim 10, wherein the storage control unit encrypts the original information using a key that exists in the secure module, and stores the encrypted original information as the second information into the memory. Jablon, column 9 lines 13-20 and 19 lines 23-44, discloses a method of storing the modification code encrypted as a second information in the memory, wherein the original information is the previously computed code. Moreover, Asokan discloses a similar method wherein the original data is stored encrypted in the memory as second information.

Asokan discloses a method wherein the second information is stored encrypted in the memory wherein the decryption key is stored in a secured memory ([0028] and [0030]. It would have been obvious to modify Jablon in view of Osborn to include the method of storing the second information in encrypted form. Motivation for doing so would have been to secure data in the non-secure memory as suggested by Asokan and as would have been obvious to one of ordinary skill in the art.

35. Claim 32 is rejected because it discloses substantially similar subject matter to claim 12.

36. Claims13-16 and 33-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon (US Patent 5421006) in view of Asokan et al. (US PgPub 2003/0076957).

37. As per claim 13, Jablon discloses the information reproducing apparatus according to claim 1, further comprising: a key managing unit that is loaded on the secure module, wherein the key managing unit holds a key used to encrypt or decode the second information, and the key managing unit supplies the key to the storage control unit, if the falsification checking unit does not detect a falsification (column 9 lines 13-20 and 19 lines 23-44). Jablon does not specifically disclose wherein the key is used to encrypt/decrypt the second information, instead a key is used to encrypt/decrypt the modification code.

Asokan discloses a similar method wherein the second information is stored in memory encrypted wherein the key is stored in secured memory wherein upon checking of the integrity code, the key is supplied to decrypt the information ([0028] and [0030]). Motivation for modifying Jablon as discussed above would have been to encrypt the second information so as to enhance security of the information in the non-secure memory as would have been readily apparent to one of ordinary skill in the art.

38. As per claim 14, Jablon in view of Asokan disclose the information reproducing apparatus according to claim 13, but does not explicitly disclose wherein the key supplied by the key managing unit is valid only for a predefined period of time. The

examiner argues that this is a well-known and common feature in the art as would have been readily apparent to one of ordinary skill, thus it would have been obvious at the time of the invention to include wherein the key is valid for only a predefined period of time. Motivation for limited use-keys is to enhance the security of the key against brute force attacks, wherein a limited-use key may be valid for too short of time to be discovered, as is well known in the art.

39. As per claim 15, Jablon in view of Asokan disclose the information reproducing apparatus according to claim 13, but do not disclose wherein the key managing unit changes the key each time the key managing unit supplies the key to the storage control unit. The examiner argues it to be a well-known and commonly performed feature in the art, wherein a key is a single use key. Single use keys are commonly implemented in the art to enhance security by preventing a reuse of an intercepted key, as would have been well known and understood to one of ordinary skill at the time of the invention.

40. As per claim 16, Jablon in view of Asokan disclose the information reproducing apparatus according to claim 13, wherein when the falsification checking unit detects a falsification, the key managing unit does not supply the key to the storage control unit (Asokan [0028] and [0030] wherein it is an implied necessary feature).

41. Claims 33-36 are rejected because they disclose substantially similar subject matter to claims 13-16 respectively.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brandon S Bludau
Examiner
Art Unit 2132

BB
***

Benjamin E. Lanier
Examiner Art 2132